PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-056037
(43)Date of publication of application : 05.03.1993

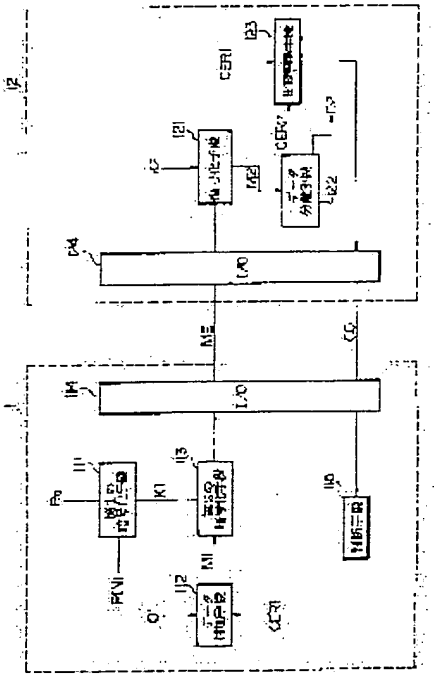
(51)Int.Cl. H04L 9/28
G06K 17/00
G09C 1/00

(21)Application number : 03-240374
(22)Date of filing : 27.08.1991

(71)Applicant : TOPPAN PRINTING CO LTD
(72)Inventor : TAKAHASHI MASASHI
YORIMOTO GIICHI
YURA AKIYUKI

(54) DATA PROCESSING SYSTEM

(57)Abstract:
PURPOSE: To reduce the processing time without deteriorating the secrecy of data in the data transmission system between an IC card and a terminal equipment.
CONSTITUTION: A password PIN1 inputted by a carrier of an IC card 12 is ciphered according to a predetermined key data Rd to generate a key data K1. A synthesis text data M1 resulting from adding an additional data CER1 to a text data D1 representing a deposit balance or the like is ciphered according to the key data K1 to generate a ciphered text data ME. The ciphered synthesis text data ME has information comprising the text data D1 and the password PIN1. The ciphered synthesis text data ME is decoded and separated into a text data D2 and an additional data CER2. The separated additional data CER2 is compared with the additional data CER1 stored in advance in the IC card 12. As a result, the adequacy of the correlation PIN1 and the text data D2 is judged. Then the number of times of ciphering/decoding and the number of times of data transmission reception between the terminal equipment 11 and the IC card 12 are reduced to reduce the time required for session.



LEGAL STATUS

[Date of request for examination] 22.06.1998
[Date of sending the examiner's decision of rejection] 16.10.2001
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] By enciphering wording-of-a-telegram data with transmitting-side equipment, transmitting the this enciphered wording-of-a-telegram data to receiving-side equipment, and decrypting the wording-of-a-telegram data this enciphered with receiving-side equipment In the data-processing method which sends and receives these wording-of-a-telegram data the above-mentioned transmitting-side equipment A data addition means to add discernment data to the above-mentioned wording-of-a-telegram data, and to generate synthetic wording-of-a-telegram data, The 1st encryption means which enciphers with the 1st key data which was able to define the password code beforehand, and generates the 2nd key data, While having the 2nd encryption means which enciphers the above-mentioned synthetic wording-of-a-telegram data with the key data of the above 2nd, and generates code composition wording-of-a-telegram data, and a transmitting means to transmit the above-mentioned code composition wording-of-a-telegram data to the above-mentioned receiving-side equipment A receiving means to receive the code composition wording-of-a-telegram data with which the above-mentioned receiving-side equipment was transmitted from the above-mentioned transmitting means, A decryption means to decrypt the above-mentioned code composition wording-of-a-telegram data according to the 3rd key data corresponding to the key data of the above 2nd, and to generate decode composition wording-of-a-telegram data, A data separation means to divide the above-mentioned decode composition wording-of-a-telegram data into decode wording-of-a-telegram data and decode discernment data, When the above-mentioned decode addition data are compared with the above-mentioned addition data and the above-mentioned decode addition data and the above-mentioned addition data are in agreement, the above-mentioned password code, And it is the data-processing method characterized by having a comparative judgment means to judge that the above-mentioned password code and the above-mentioned decode wording-of-a-telegram data are inaccurate when it judges that the above-mentioned decode wording-of-a-telegram data are just and the above-mentioned decode addition data and the above-mentioned addition data are not in agreement.
[Claim 2] The key data of the above 3rd are a data-processing method according to claim 1 characterized by it being generated beforehand and coming to be held with an authorization code and the 1st key data at the store of the above-mentioned receiving-side equipment.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to a data-processing method and the data-processing method which protects the confidentiality of the commo data used in an IC card and a card data processor in detail.
[0002]
[Description of the Prior Art] Conventionally, in the field of an information communication link, techniques, such as encryption of communication link wording of a telegram and electronic signature, have been used as a means to prevent the so-called security risks, such as tapping of the communication link wording of a telegram by the malfeasance, and forgery. For example, data-processing methods, such as "the approach of transmitting secret data between a sending set and a receiving set, equipment", etc. which are shown in the open patent official report No. 136058 [Showa 56 to], have been thought out.
[0003] Drawing 3 is the outline block diagram showing an example of such a conventional data-processing method. This data-processing method has a terminal (transmitting side) 31 and IC card (receiving side) 32, and is constituted. If, as for this data-processing method, IC card 32 holder inputs the password code PIN 1 into a terminal 31, the wording-of-a-telegram data D1, such as the deposits-and-savings balance, will be written in IC card 32 as wording-of-a-telegram data D2 at IC card 32.
[0004] In a terminal 31, the standard key data R which can change the value at random are enciphered by the encryption means 311, and the proper key data R1 are generated. It is transmitted by the transceiver means 316 and this standard key data R is inputted into the encryption means 321 through the transceiver means 326 of IC card 32. This encryption means 321 generates the proper key data R2 based on the standard key data R.
[0005] By changing this standard key data R into each session (data communication between a terminal and an IC card) of every at random, it made it difficult that the proper key data R1 and R2 were known by the third party, and unjust acts, such as tapping of wording-of-a-telegram data D1 grade and forgery of IC card 32, are prevented. Moreover, also when the proper key data R1 and R2 are known by the third party in a certain session, since the standard key data R are changed at random, even the proper key data R1 and R2 in other sessions should not be known.
[0006] Then, in a terminal 31, the password code PIN 1 is enciphered considering the above-mentioned proper key data R1 as a key by the encryption means 312, and the code password code AV1 is generated. This code password code AV1 is inputted into the decryption means 322 through the transceiver means 316 and the transceiver means 326. Then, the code password code AV1 is decrypted considering the above-mentioned proper key data R2 as a key, and the password code PIN 2 is generated. The comparison means 323 compares the decrypted password code PIN 2 with the password code PIN 1 in which it was beforehand stored by IC card 32. And as a result of meaning whether the password code PIN 2 is in agreement with the password code PIN 1, IC card 32 outputs data C1 to a terminal 31.
[0007] The result data C1 are inputted into the decision means 313 through the transceiver means 326 and 316. When it is judged that the password code PIN 2 of the decision means 313 does not correspond with the password code PIN 1 from the result data C1, the session concerned is interrupted and IC card 32 is discharged from a terminal 31. On the other hand, when the password code PIN 2 was in agreement with the password code PIN 1 and the decision means 313 judges, it is carried out by the next processing continuing.
[0008] The wording-of-a-telegram data D1 are enciphered by the encryption means 314 by using the above-mentioned proper key data R1 as a key, and the encryption wording-of-a-telegram data DE are generated. The encryption wording-of-a-telegram data DE are inputted into the decryption means 324 through the transceiver means 316 and 326. The encryption wording-of-a-telegram data DE are decrypted by the decryption means 324 by using the above-mentioned proper key data R2 as a key, and the wording-of-a-telegram data D2 are generated.
[0009] The wording-of-a-telegram data D2 are written in the memory in IC card 32 (not shown). The decision means 325 judges whether processing of the writing of the wording-of-a-telegram data D2 etc. was performed normally, and transmits the result data C2 to the decision means 315 through the transceiver means 315 and 326. As a result of decision, if processing of the writing of the wording-of-a-telegram data D2 etc. is normal, the session processing concerned will be ended, and if not normal, IC card 32 will be discharged from a terminal 31.
[0010] In addition, in the above-mentioned encryption means 312 and 314 and the decryption means 322 and 324, encryption algorithms, such as DES (Data Encryption Standard), FEAL, and RSA, are used.
[0011]

[Problem(s) to be Solved by the Invention] However, in the conventional data-processing method, CPU of the comparatively late 8-bit class of processing speed is mainly carried in the IC card which is a receiving side from constraint of mounting space etc. For this reason, when processing shown in the data-processing method concerning the above-mentioned conventional technique was performed, there was a problem that it was not suitable for practical use that there are many counts of that there are many counts of transmission of wording-of-a-telegram data, encryption, and a decryption in order to require long duration (several seconds) as that processing time as a whole. Moreover, for the object which shortens the processing time, when a simple method realized a data-processing method, the confidentiality of data, such as wording-of-a-telegram data, an authorization code, and proper key data, fell, and the problem of becoming easy to generate a security risk had arisen.
[0012]
[Objects of the Invention] Then, this invention sets it as the object to offer the data-processing method which can shorten the processing time, without reducing the confidentiality of data.
[0013]
[Means for Solving the Problem] The data-processing method concerning invention according to claim 1 By enciphering wording-of-a-telegram data with transmitting-side equipment, transmitting the this enciphered wording-of-a-telegram data to receiving-side equipment, and decrypting the wording-of-a-telegram data this enciphered with receiving-side equipment In the data-processing method which sends and receives these wording-of-a-telegram data the above-mentioned transmitting-side equipment A data addition means to add discernment data to the above-mentioned wording-of-a-telegram data, and to generate synthetic wording-of-a-telegram data, The 1st encryption means which enciphers with the 1st key data which was able to define the password code beforehand, and generates the 2nd key data, While having the 2nd encryption means which enciphers the above-mentioned synthetic wording-of-a-telegram data with the key data of the above 2nd, and generates code composition wording-of-a-telegram data, and a transmitting means to transmit the above-mentioned code composition wording-of-a-telegram data to the above-mentioned receiving-side equipment A receiving means to receive the code composition wording-of-a-telegram data with which the above-mentioned receiving-side equipment was transmitted from the above-mentioned transmitting means, A decryption means to decrypt the above-mentioned code composition wording-of-a-telegram data according to the 3rd key data corresponding to the key data of the above 2nd, and to generate decode composition wording-of-a-telegram data, A data separation means to divide the above-mentioned decode composition wording-of-a-telegram data into decode wording-of-a-telegram data and decode discernment data, When the above-mentioned decode addition data are compared with the above-mentioned addition data and the above-mentioned decode addition data and the above-mentioned addition data are in agreement, the above-mentioned password code, And when it judges that the above-mentioned decode wording-of-a-telegram data are just and the above-mentioned decode addition data and the above-mentioned addition data are not in agreement, it is the data-processing method characterized by having the above-mentioned password code and a comparative judgment means to judge that the above-mentioned decode wording-of-a-telegram data are inaccurate.
[0014] Data-processing method concerning invention according to claim 2 It is the data-processing method according to claim 1 characterized by the key data of the above 3rd being generated beforehand and coming to hold them with an authorization code and the 1st key data at a store.
[0015]
[Function] In a transmitting side, the data-processing method concerning invention according to claim 1 enciphers an authorization code according to the 1st (determined according to card) key data defined beforehand, and generates the 2nd key data. Moreover, addition data are added to the wording-of-a-telegram data in which the content which should be transmitted is shown, and synthetic wording-of-a-telegram data are generated. And this synthetic wording-of-a-telegram data is enciphered based on the key data of the above 2nd, and code composition wording-of-a-telegram data are generated. This code composition wording-of-a-telegram data is transmitted to a receiving side through a transmitting means.
[0016] In a receiving side, the above-mentioned code composition wording-of-a-telegram data are received through a receiving means. This code composition wording-of-a-telegram data is decrypted with the 3rd key data, and generates decode composition wording-of-a-telegram data. This decode composition wording-of-a-telegram data is divided into decode wording-of-a-telegram data and decode discernment data. When this decode discernment data is compared with the above-mentioned discernment data and the above-mentioned decode discernment data and the above-mentioned discernment data are in agreement, it is judged that the above-mentioned authorization code and the above-mentioned decode wording-of-a-telegram data are just. Then, this wording-of-a-telegram data will be written in the IC card which is receiving-side equipment, for example. On the contrary, when the above-mentioned decode discernment data and the above-mentioned discernment data are not in agreement, it is judged that the above-mentioned authorization code and the above-mentioned decode wording-of-a-telegram data are inaccurate. In this case, wording-of-a-telegram data are not written in an IC card.
[0017] Thus, in order to encipher wording-of-a-telegram data with discernment data and to transmit, the routine which transmits only an authorization code apart from transmission of wording-of-a-telegram data, and performs the authentication like before can be omitted, and the effectiveness of transmission of wording-of-a-telegram data is raised. Moreover, since discernment data and wording-of-a-telegram data are enciphered and decrypted simultaneously, the step of encryption and a decryption also decreases compared with the conventional case, and the effectiveness of the data transmission processing is raised. Furthermore, since the authorization code of a proper was used for the receiving side in this case and wording-of-a-telegram data are enciphered, the security

about wording-of-a-telegram data which transmits is raised even to the same extent as the case where it is presupposed that the conventional standard key is changed for every session.
[0018] Data-processing method concerning invention according to claim 2 With an authorization code and the 1st key data, the key data of the above 3rd are generated beforehand and held at the storage of the above-mentioned receiving-side equipment. For this reason, it is not necessary to transmit the key data of the above 3rd to receiving-side equipment from transmitting-side equipment, and the time amount which a session takes can be shortened.
[0019]
[Example] Below, the example of this invention is explained, referring to a drawing.
[0020] Drawing 1 is the block diagram showing the outline of the data-processing method concerning the 1st example of this invention. This data-processing method has a terminal (transmitting side) 11 and IC card (receiving side) 12, and is constituted. This example explains the case where the terminal by which online connection was made considering for example, the ATM card for banks as a terminal at the host computer of a bank is used as IC card 12. In this case, an authorization code shall be the thing of a different proper for every card, and only the card holder shall know it. Therefore, hereafter, a card holder inputs authorization code PIN1 into a terminal 31, a terminal performs further predetermined actuation, and the case where the credit of the fixed amount of money is drawn out is explained. Credit cash-drawer processing needs to be performed with a terminal and a host computer, and the credit balance needs to calculate it, and it needs to write this credit balance in a card. Consequently, the wording-of-a-telegram data D1 in which the credit balance and its writing are shown from a host computer are transmitted to a terminal 31, and a terminal transmits this wording-of-a-telegram data to an IC card.
[0021] In the terminal 11 which constitutes transmitting-side equipment, it has the 1st encryption means 11. This 1st encryption means 11 enciphers inputted authorization code PIN1 according to the key data Rd which are the code of the secrecy determined at the time of card issuance, and generates the key data K1. Moreover, this 1st encryption means 11 is constituted by using the encryption algorithm exhibited [RSA / DES, FEAL,].
[0022] Moreover, a terminal 11 adds the discernment data CER1 to the above-mentioned wording-of-a-telegram data D1, has a data addition means 112 to generate the synthetic wording-of-a-telegram data M1, the 2nd encryption means 113 which enciphers the synthetic wording-of-a-telegram data M1, and generates the code composition wording-of-a-telegram data ME, and the transceiver means (I/O circuit) 114 which transmit and receive data between IC cards 12, and is constituted. The same open mold encryption algorithm as the encryption means of the above 1st also constitutes the 2nd encryption means 113.
[0023] On the other hand, IC card 12 is constituted including 8-bit CPU etc., and this CPU is performing processing shown by the following processing means. Namely, a transceiver means 124 by which IC card 12 transmits and receives data between terminals 11 (I/O circuit), A decryption means 121 to decrypt code composition wording-of-a-telegram data according to the key data K2 which were able to be defined beforehand, and to generate the synthetic wording-of-a-telegram data M2, A data separation means 122 to divide the synthetic wording-of-a-telegram data M2 into the wording-of-a-telegram data D2 and the discernment data CER2, The discernment data CER2 are compared with the discernment data CER1, and authorization code PIN1 and the wording-of-a-telegram data M2 have a comparative judgment means 123 to judge whether it is the right, and are constituted. Furthermore, although not illustrated, this IC card 12 has EEPROM in which data, such as the above-mentioned credit balance, were stored, and is constituted.
[0024] The above-mentioned decryption means 121 can process the inverse function of the above-mentioned encryption means 113, and these decryption means 121 and the encryption means 113 can use encryption algorithms, such as DES, FEAL, and RSA, like the above. Moreover, the processing in the above-mentioned data addition means 112 and the data separation means 122 may use what kind of mode of processing, as long as the wording-of-a-telegram data D2 and the discernment data CER2 are disengageable.
[0025] In addition, the above-mentioned terminal has the decision means 115, this decision means judges forward [of wording-of-a-telegram data and an authorization code], and injustice based on the response from the above-mentioned IC card, for example, when inaccurate, a right case orders it the blowdown processing from the terminal of the IC card concerned etc., while outputting that to a host computer.
[0026] Next, an operation of the data-processing method concerning this example is explained, referring to the flow chart of drawing 2 . In this flow chart, S201-S204 show the processing by the side of a terminal 11, and S205-S211 show the processing by the side of an IC card.
[0027] Authorization code PIN1 is inputted into a terminal 11 by the IC card holder. According to the key data Rd determined at the time of card issuance, it enciphers with the encryption means 111, and authorization code PIN1 generates the key data K1 (S201). And about the wording-of-a-telegram data D1 in which the credit balance from a host computer etc. is shown, the discernment data CER1 are added to the wording-of-a-telegram data D1 with the data addition means 112 (for example, a parity bit is added), and the synthetic wording-of-a-telegram data M1 are generated (S202).
[0028] Furthermore, this synthetic wording-of-a-telegram data M1 is enciphered according to the above-mentioned key data K1, and the code composition wording-of-a-telegram data ME are generated (S203). This code composition wording-of-a-telegram data ME is transmitted to IC card 12 through the transceiver means 114 (S204). Consequently, IC card 12 receives this code composition wording-of-a-telegram data through the transceiver means 124.
[0029] The received code composition wording-of-a-telegram data ME are decrypted by the decryption means 121

according to the key data K2, and the synthetic wording-of-a-telegram data M2 are generated (S205). The key data K2 have the value corresponding to the above-mentioned key data K1, and the decryption means 121 performs decryption processing according to the operations sequence of the above-mentioned encryption means 113 and reverse. In addition, the key data K2 can also use data equivalent to the above-mentioned key data K1, and you may make it receive this key data K2 from a terminal 11 after session initiation by using the encryption algorithm of object key methods, such as DES. Furthermore, the key data K2 enciphered with the key data Rd which are the 1st key data beforehand set up according to each card in the authorization code (personal identification number) which may store in IC card 12 the value defined at the time of issuance of IC card 12, for example, is inputted at the time of each card issuance may be beforehand stored in IC card 12. Since the count of transmission and reception of the data of a terminal 11 and IC card 12 becomes fewer when the key data K2 are stored in IC card 12, much more high-speed processing can be aimed at.

[0030] Furthermore, this synthetic wording-of-a-telegram data M2 is separated into the wording-of-a-telegram data D2 and the discernment data CER2 by the data separation means 122 (S206). The comparative judgment means 123 compares the separated discernment data CER2 with the discernment data CER1 in which it was stored by IC card 12 at the time of IC card issuance (S207). In addition, the discernment data CER1 stored in IC card 12 are equivalent to the discernment data CER1 stored in the above-mentioned terminal 11.

[0031] As a result of a comparison, when the separated discernment data CER2 are in agreement with the discernment data CER1, YES), above-mentioned authorization code PIN1, and the wording-of-a-telegram data D2 are judged to be the rights by (S207 (S208). Consequently, as a result of showing normal processing, the wording-of-a-telegram data D2 in which this credit balance is shown transmit data C0 to the transceiver means 114 through the transceiver means 124, while being written in EEPROM of IC card 12 (S209). As a result, the decision means 115 terminates the session of IC card 12 and a terminal 11 according to data C0.

[0032] As a result of a comparison, when the separated discernment data CER2 are not in agreement with the discernment data CER1, it is judged by (S207 that NO), above-mentioned authorization code PIN1, and the wording-of-a-telegram data D2 are not right (S210). That is, authorization code PIN1 judges that the not an authorization code but wording-of-a-telegram data D2 of IC card 12 in the session concerned differ from the wording-of-a-telegram data D1 as a result processed with the host computer. Therefore, without writing this wording-of-a-telegram data D2 in IC card 12, as a result of showing exception processing, data C0 are transmitted to the transceiver means 114 through the transceiver means 124. Consequently, the decision means 115 discharges IC card 12 from a terminal 11 (S211), and a session is terminated. Consequently, the unjust writing to IC card 12 is prevented.

[0033] As mentioned above, as explained, in this example, it enciphers according to the key data K1 which generated the wording-of-a-telegram data D1 from authorization code PIN1, and the code composition wording-of-a-telegram data ME are generated. Therefore, in addition to the wording-of-a-telegram data D1, the code composition wording-of-a-telegram data ME will also have the information on authorization code PIN1. For this reason, the data-processing method concerning this example does not need to perform encryption and a decryption for authorization code PIN1 and the wording-of-a-telegram data D1 independently, as performed by the conventional data-processing method. Moreover, as compared with the conventional data-processing method, transmission and reception of the data between a terminal and an IC card decrease from 4 times to 2 times, and the count of encryption and a decryption is decreasing the data-processing method concerning this example from 6 times to 2 times. Therefore, according to this example, the time amount which the session between a terminal and an IC card takes can be substantially decreased from Number sec to hundreds msec(s).

[0034] Moreover, the key data K1 are generated by enciphering different authorization code PIN1 for every IC card. For this reason, since the key data K1 of other IC cards 12 will not be known even if authorization code PIN1 of IC card 12 of one sheet is known by the third party, the confidentiality of the data of other IC cards 12 does not fall. Therefore, it is not spoiled to the confidentiality of the data of other IC cards, and the damage by the so-called security risk can be suppressed to the minimum. Furthermore, also when a third party acquires others' IC card 12, if a third party does not know the authorization code of this IC card, the data encryption and the decryption are impossible.

[0035] Therefore, the data-processing method concerning this example can shorten the time amount which a session takes, without reducing the confidentiality of data as compared with the conventional data-processing method.

[0036]

[Effect of the Invention] The data-processing method which can shorten the processing time can be offered without reducing the confidentiality of data according to this invention, as explained above.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the outline block diagram showing the data-processing method concerning the 1st example of this invention.
[Drawing 2] It is the flow chart which shows actuation of the data-processing method concerning the 1st example of this invention.
[Drawing 3] It is the outline block diagram showing an example of the conventional data-processing method.
[Description of Notations]
11 Terminal System (Transmitting Side)
12 IC Card (Receiving Side)
111 1st Encryption Means
112 Data Addition Means
113 2nd Encryption Means
114 Transceiver Means (Transmitting Means)
121 Decryption Means
122 Data Separation Means
123 Comparative Judgment Means
124 Transceiver Means (Receiving Means)
D1 Wording-of-a-telegram data
D2 Wording-of-a-telegram data (decode wording-of-a-telegram data)
PIN1 Authorization code
CER1 Discernment data
CER2 Discernment data (decode discernment data)
M1 Synthetic wording-of-a-telegram data
M2 Synthetic wording-of-a-telegram data (decode composition wording-of-a-telegram data)
Rd Key data (1st key data)
K1 Key data (2nd key data)
K2 Key data (3rd key data)

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平5－56037

(43)公開日　平成5年(1993)3月5日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ04Ｌ　9/28				
Ｇ06Ｋ　17/00		F　8623－5L		
Ｇ09Ｃ　1/00		7922－5L		
		7117－5K	Ｈ04Ｌ　9／02	A

審査請求　未請求　請求項の数2(全　8　頁)

(21)出願番号　特願平3－240374

(22)出願日　平成3年(1991)8月27日

(71)出願人　000003193
凸版印刷株式会社
東京都台東区台東1丁目5番1号

(72)発明者　高橋　正志
東京都台東区台東一丁目5番1号　凸版印刷株式会社内

(72)発明者　寄本　義一
東京都台東区台東一丁目5番1号　凸版印刷株式会社内

(72)発明者　由良　彰之
東京都台東区台東一丁目5番1号　凸版印刷株式会社内

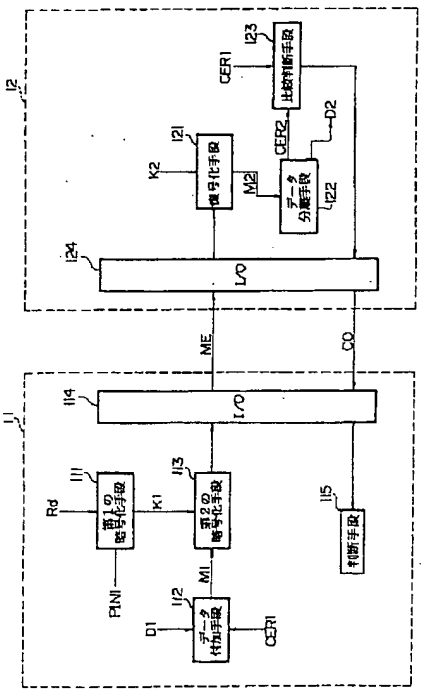
(74)代理人　弁理士　桑井　清一

(54)【発明の名称】　データ処理方式

(57)【要約】

【目的】　ＩＣカードと端末とのデータ伝送方式において、データの機密性を低下させることなく処理時間を短縮する。

【構成】　ＩＣカード１２保持者が入力した暗証コードＰＩＮ１を予め定めた鍵データＲｄに従い暗号化し、鍵データＫ１を生成する。預金残高等をあらわす電文データＤ１に付加データＣＥＲ１を付加した合成電文データＭ１を、鍵データＫ１に従い暗号化し、暗号電文データＭＥを生成する。この暗号合成電文データＭＥは、電文データＤ１と暗証コードＰＩＮ１との情報を有する。暗号合成電文データＭＥを復号化し、さらに電文データＤ２と付加データＣＥＲ２に分離する。分離した付加データＣＥＲ２を、予めＩＣカード１２に格納された付加データＣＥＲ１と比較する。この結果により、暗証コードＰＩＮ１と電文データＤ２との正当性を判断する。よって、暗号化・復号化の回数、および、端末１１とＩＣカード１２とのデータの送受信の回数を減少させ、セッションに要する時間を短縮する。



1

【特許請求の範囲】

【請求項１】　送信側装置で電文データを暗号化し、該暗号化された電文データを受信側装置に送信し、受信側装置では該暗号化された電文データを復号化することにより、該電文データを送受するデータ処理方式において、

上記送信側装置は、上記電文データに識別データを付加し、合成電文データを生成するデータ付加手段と、

暗証コードを予め定められた第１の鍵データにより暗号化し、第２の鍵データを生成する第１の暗号化手段と、

上記合成電文データを、上記第２の鍵データにより暗号化し暗号合成電文データを生成する第２の暗号化手段と、

上記暗号合成電文データを上記受信側装置に送信する送信手段と、を有するとともに、

上記受信側装置は、上記送信手段から送信された暗号合成電文データを受信する受信手段と、

上記暗号合成電文データを、上記第２の鍵データに対応した第３の鍵データに従い復号化し、復号合成電文データを生成する復号化手段と、

上記復号合成電文データを、復号電文データと復号識別データとに分離するデータ分離手段と、

上記復号付加データと上記付加データとを比較し、上記復号付加データと上記付加データとが一致する場合には上記暗証コード、および、上記復号電文データは正当であると判断し、上記復号付加データと上記付加データとが一致しない場合には上記暗証コード、および、上記復号電文データは不正であると判断する比較判断手段と、を有することを特徴とするデータ処理方式。

【請求項２】　上記第３の鍵データは、認証コードと第１の鍵データにより、予め生成され、上記受信側装置の記憶装置に保持されてなることを特徴とする請求項１記載のデータ処理方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はデータ処理方式、詳しくはＩＣカードとカードデータ処理装置において使用される通信データの機密性を保護するデータ処理方式に関する。

【０００２】

【従来の技術】従来、情報通信の分野において、不正行為による通信電文の盗聴、偽造等のいわゆるセキュリティ・リスクを防止する手段として通信電文の暗号化、電子署名等の技術が用いられてきた。例えば、公開特許公報昭５６－１３６０５８号に示す「送信装置および受信装置間で機密データを電送する方法および装置」等のようなデータ処理方式が案出されてきた。

【０００３】図３は、このような従来のデータ処理方式の一例を示す概略ブロック図である。このデータ処理方式は、例えば端末（送信側）３１と、ＩＣカード（受信側）３２とを有して構成されている。このデータ処理方式は、ＩＣカード３２保持者が暗証コードＰＩＮ１を端末３１に入力すると、預貯金残高等の電文データＤ１がＩＣカード３２に電文データＤ２としてＩＣカード３２に書き込まれるものである。

2

【０００４】端末３１においては、ランダムにその値を変更し得る標準鍵データＲが暗号化手段３１１により暗号化され、固有鍵データＲ１が生成される。この標準鍵データＲは送受信手段３１６により送信され、ＩＣカード３２の送受信手段３２６を介して暗号化手段３２１に入力される。この暗号化手段３２１は、標準鍵データＲに基づいて固有鍵データＲ２を生成する。

【０００５】この標準鍵データＲを各セッション（端末とＩＣカードとの間のデータ通信）毎にランダムに変更することにより、固有鍵データＲ１，Ｒ２が第三者に知られることを困難にし、電文データＤ１等の盗聴、ＩＣカード３２の偽造等の不正な行為を防止している。また、万一、あるセッションにおいて固有鍵データＲ１、Ｒ２が第三者に知られた場合にも、標準鍵データＲはランダムに変更されるため、他のセッションにおける固有鍵データＲ１、Ｒ２まで知られることはない。

【０００６】続いて、端末３１においては、暗証コードＰＩＮ１は暗号化手段３１２により、上記固有鍵データＲ１を鍵として暗号化され、暗号暗証コードＡＶ１が生成される。この暗号暗証コードＡＶ１は、送受信手段３１６、送受信手段３２６を介して復号化手段３２２に入力される。すると、暗号暗証コードＡＶ１は、上記固有鍵データＲ２を鍵として復号化され、暗証コードＰＩＮ２が生成される。復号化された暗証コードＰＩＮ２を、比較手段３２３は、予めＩＣカード３２に格納されていた暗証コードＰＩＮ１と比較する。そして、暗証コードＰＩＮ２が暗証コードＰＩＮ１と一致しているかどうかをあらわす結果データＣ１をＩＣカード３２は端末３１に出力する。

【０００７】結果データＣ１は、送受信手段３２６、３１６を介して判断手段３１３に入力される。判断手段３１３は、結果データＣ１より暗証コードＰＩＮ２が暗証コードＰＩＮ１と一致しないと判断した場合には、当該セッションを中断し、ＩＣカード３２を端末３１から排出する。一方、暗証コードＰＩＮ２が暗証コードＰＩＮ１に一致していると判断手段３１３が判断した場合には、次の処理が続いて行われる。

【０００８】電文データＤ１は、上記固有鍵データＲ１を鍵として暗号化手段３１４により暗号化され、暗号化電文データＤＥが生成される。暗号化電文データＤＥは、送受信手段３１６、３２６を介して復号化手段３２４に入力される。暗号化電文データＤＥは、上記固有鍵データＲ２を鍵として復号化手段３２４により復号化され、電文データＤ２が生成される。

【０００９】電文データＤ２は、ＩＣカード３２内のメ

モリ（図示されていない）に書き込まれる。判断手段３２５は、電文データＤ２の書き込み等の処理が正常に行われたかどうかを判断し、結果データＣ２を送受信手段３１５、３２６を介して判断手段３１５に送信する。判断の結果、電文データＤ２の書き込み等の処理が正常であれば当該セッション処理を終了し、正常でなければＩＣカード３２を端末３１から排出する。

【００１０】なお、上記暗号化手段３１２、３１４、復号化手段３２２、３２４においては、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）、ＦＥＡＬ、ＲＳＡ等の暗号化アルゴリズムが用いられている。

【００１１】

【発明が解決しようとする課題】しかしながら、従来のデータ処理方式においては、受信側であるＩＣカードには、実装空間等の制約から処理速度の比較的遅い８ビットクラスのＣＰＵが主に搭載されている。このため、上記従来技術に係るデータ処理方式に示される処理を行った場合、電文データの伝送回数が多いこと、暗号化、復号化の回数が多いことにより、全体としてその処理時間として長時間（数秒）を要するため、実用に適しないという問題があった。また、処理時間を短縮する目的により、データ処理方式を簡易な方式にて実現した場合に、電文データ、認証コード、固有鍵データ等のデータの機密性が低下し、セキュリテイ・リスクが発生しやすくなるという問題が生じていた。

【００１２】

【発明の目的】そこで、本発明はデータの機密性を低下させることなく処理時間を短縮できるデータ処理方式を提供することをその目的としている。

【００１３】

【課題を解決するための手段】請求項１に記載の発明に係るデータ処理方式は、送信側装置で電文データを暗号化し、該暗号化された電文データを受信側装置に送信し、受信側装置では該暗号化された電文データを復号化することにより、該電文データを送受するデータ処理方式において、上記送信側装置は、上記電文データに識別データを付加し、合成電文データを生成するデータ付加手段と、暗証コードを予め定められた第１の鍵データにより暗号化し、第２の鍵データを生成する第１の暗号化手段と、上記合成電文データを、上記第２の鍵データにより暗号化し暗号合成電文データを生成する第２の暗号化手段と、上記暗号合成電文データを上記受信側装置に送信する送信手段と、を有するとともに、上記受信側装置は、上記送信手段から送信された暗号合成電文データを受信する受信手段と、上記暗号合成電文データを、上記第２の鍵データに対応した第３の鍵データに従い復号化し、復号合成電文データを生成する復号化手段と、上記復号合成電文データを、復号電文データと復号識別データとに分離するデータ分離手段と、上記復号付加データと上記付加データとを比較し、上記復号付加データと

上記付加データとが一致する場合には上記暗証コード、および、上記復号電文データは正当であると判断し、上記復号付加データと上記付加データとが一致しない場合には上記暗証コード、および、上記復号電文データは不正であると判断する比較判断手段と、を有することを特徴とするデータ処理方式である。

【００１４】請求項２記載の発明に係るデータ処理方式は　上記第３の鍵データは、認証コードと第１の鍵データにより、予め生成され、記憶装置に保持されてなることを特徴とする請求項１記載のデータ処理方式である。

【００１５】

【作用】請求項１記載の発明に係るデータ処理方式は、送信側においては、予め定められた（カードに応じて決定される）第１の鍵データに従い認証コードを暗号化して、第２の鍵データを生成する。また、送信すべき内容を示す電文データには付加データを付加し、合成電文データを生成する。そして、この合成電文データを上記第２の鍵データに基づいて暗号化し、暗号合成電文データを生成する。この暗号合成電文データは、送信手段を介して受信側に送信される。

【００１６】受信側においては、受信手段を介して上記暗号合成電文データを受信する。この暗号合成電文データは、第３の鍵データにより復号化され、復号合成電文データを生成する。この復号合成電文データは、復号電文データと、復号識別データとに分離される。この復号識別データと上記識別データとを比較し、上記復号識別データと上記識別データとが一致する場合には、上記認証コード、および、上記復号電文データは正当であると判断する。この後、例えばこの電文データは受信側装置であるＩＣカードに書き込まれることとなる。逆に、上記復号識別データと上記識別データとが一致しない場合には、上記認証コード、および、上記復号電文データは不正であると判断する。この場合は電文データをＩＣカードに書き込まない。

【００１７】このように、電文データを識別データとともに暗号化して送信するため、従来のように、電文データの送信とは別に認証コードのみを送信してその認証を行うルーチンを省略することができ、電文データの送信の効率が高められている。また、識別データと電文データとを同時に暗号化、復号化しているため、暗号化、復号化のステップも、従来の場合に比べて少なくなり、そのデータ伝送処理の効率が高められる。さらに、この場合、受信側に固有の認証コードを用いて電文データを暗号化しているため、送信する電文データについてのセキュリティは従来の標準キーをセッション毎に変更するとした場合と同様の程度にまで高められている。

【００１８】請求項２記載の発明に係るデータ処理方式は　上記第３の鍵データは、認証コードと第１の鍵データにより、予め生成され、上記受信側装置の記憶装置に保持されている。このため、送信側装置から受信側装置

5

への上記第３の鍵データの送信を行う必要がなく、セッションに要する時間を短縮することができる。

【００１９】

【実施例】以下に、本発明の実施例を図面を参照しながら説明する。

【００２０】図１は、本発明の第１実施例に係るデータ処理方式の概略を示すそのブロック図である。このデータ処理方式は、例えば端末（送信側）１１と、ＩＣカード（受信側）１２とを有して構成されている。この実施例では、ＩＣカード１２として例えば銀行用キャッシュカードを、端末としては銀行のホストコンピュータにオンライン接続された端末を、用いた場合について説明する。この場合、認証コードはカード毎に異なる固有のものであり、カード保持者のみが知っているものとする。したがって、以下、カード保持者が認証コードＰＩＮ１を端末３１に入力し、さらに所定の操作を端末により行い、一定金額の預金を引出した場合について説明する。預金引出し処理は端末、および、ホストコンピュータにより実行され、預金残高が演算され、この預金残高をカードに書き込む必要がある。この結果、ホストコンピュータより預金残高およびその書き込みを示す電文データＤ１が端末３１に送信され、端末はこの電文データをＩＣカードに送信するものである。

【００２１】送信側装置を構成する端末１１においては、第１の暗号化手段１１を有している。この第１の暗号化手段１１は、入力された認証コードＰＩＮ１をカード発行時に決定された秘密のコードである鍵データＲｄに従い暗号化し、鍵データＫ１を生成するものである。また、この第１の暗号化手段１１は、例えばＤＥＳ、ＦＥＡＬ、ＲＳＡ等の公開された暗号化アルゴリズムを用いることにより構成されている。

【００２２】また、端末１１は、上記電文データＤ１に識別データＣＥＲ１を付加し、合成電文データＭ１を生成するデータ付加手段１１２と、合成電文データＭ１を暗号化し、暗号合成電文データＭＥを生成する第２の暗号化手段１１３と、ＩＣカード１２との間でデータの送受信を行う送受信手段（Ｉ／Ｏ回路）１１４と、を有して構成されている。第２の暗号化手段１１３も上記第１の暗号化手段と同一の公開型暗号化アルゴリズムによって構成している。

【００２３】一方、ＩＣカード１２は、８ビットＣＰＵ等を含んで構成されており、このＣＰＵは以下の処理手段によって示される処理を行っている。すなわち、ＩＣカード１２は、端末１１との間にてデータの送受信を行う送受信手段（Ｉ／Ｏ回路）１２４と、暗号合成電文データを予め定められた鍵データＫ２に従い復号化し、合成電文データＭ２を生成する復号化手段１２１と、合成電文データＭ２を電文データＤ２と識別データＣＥＲ２とに分離するデータ分離手段１２２と、識別データＣＥＲ２と識別データＣＥＲ１とを比較し、認証コードＰＩＮ１、電文データＭ２が正しいかどうかを判断する比較判断手段１２３と、を有して構成されている。さらに、このＩＣカード１２は、図示していないが、上記預金残高等のデータが格納されたＥＥＰＲＯＭを有して構成されている。

6

【００２４】上記復号化手段１２１は、上記暗号化手段１１３の逆関数の処理を行うものであり、これらの復号化手段１２１、暗号化手段１１３は上記と同様にＤＥＳ、ＦＥＡＬ、ＲＳＡ等の暗号化アルゴリズムを用いることができる。また、上記データ付加手段１１２、データ分離手段１２２における処理は、電文データＤ２と識別データＣＥＲ２とが分離可能である限り、どのような処理方式を用いてもよい。

【００２５】なお、上記端末は判断手段１１５を有しており、この判断手段は上記ＩＣカードからのレスポンスに基づいて電文データ、認証コードの正、不正を判断して、例えば正しい場合はホストコンピュータにその旨の出力をなすとともに、不正の場合には当該ＩＣカードの端末からの排出処理等を指令する。

【００２６】次に本実施例に係るデータ処理方式の作用を図２のフローチャートを参照しながら説明する。このフローチャートにおいて、Ｓ２０１～Ｓ２０４は端末１１側の処理を示し、Ｓ２０５～Ｓ２１１はＩＣカード側の処理を示している。

【００２７】ＩＣカード保持者により認証コードＰＩＮ１が端末１１に入力される。認証コードＰＩＮ１は、カード発行時に決定された鍵データＲｄにしたがい暗号化手段１１１により暗号化し、鍵データＫ１を生成する（Ｓ２０１）。そして、ホストコンピュータからの預金残高等を示す電文データＤ１については、その電文データＤ１に識別データＣＥＲ１をデータ付加手段１１２により付加し（例えばパリティビットを付加する）、合成電文データＭ１を生成する（Ｓ２０２）。

【００２８】さらに、この合成電文データＭ１を、上記鍵データＫ１に従い暗号化し、暗号合成電文データＭＥを生成する（Ｓ２０３）。この暗号合成電文データＭＥは送受信手段１１４を介してＩＣカード１２に送信される（Ｓ２０４）。この結果、ＩＣカード１２は送受信手段１２４を介してこの暗号合成電文データを受信する。

【００２９】受信された暗号合成電文データＭＥは鍵データＫ２に従い復号化手段１２１により復号化され、合成電文データＭ２が生成される（Ｓ２０５）。鍵データＫ２は上記鍵データＫ１に対応した値を有しており、復号化手段１２１は上記暗号化手段１１３と逆の動作手順に従い復号化処理を行う。なお、ＤＥＳ等の対象鍵方式の暗号化アルゴリズムを使用することにより、鍵データＫ２は上記鍵データＫ１と等価なデータを使用することもでき、この鍵データＫ２はセッション開始後、端末１１から受信するようにしてもよい。さらに、ＩＣカード１２の発行時に定められた値をＩＣカード１２に格納し

ていてもよく、例えば各カード発行時に入力される認証コード（暗証番号）を予め各カードに応じて設定された第１の鍵データである鍵データＲｄにより暗号化された鍵データＫ２を予めＩＣカード１２に格納していてもよい。鍵データＫ２をＩＣカード１２に格納した場合には、端末１１とＩＣカード１２とのデータの送受信の回数が減るため、より一層の高速処理を図ることができる。

【００３０】さらに、この合成電文データＭ２は、データ分離手段１２２により、電文データＤ２と識別データＣＥＲ２とに分離される（Ｓ２０６）。比較判断手段１２３は、分離された識別データＣＥＲ２を、ＩＣカード発行時にＩＣカード１２に格納された識別データＣＥＲ１と比較する（Ｓ２０７）。なお、ＩＣカード１２に格納された識別データＣＥＲ１は上記端末１１に格納された識別データＣＥＲ１と等価である。

【００３１】比較の結果、分離された識別データＣＥＲ２が識別データＣＥＲ１と一致した場合には（Ｓ２０７でＹＥＳ）、上記認証コードＰＩＮ１、および、電文データＤ２は正しいと判断する（Ｓ２０８）。その結果、この預金残高を示す電文データＤ２はＩＣカード１２のＥＥＰＲＯＭに書き込まれるとともに（Ｓ２０９）、正常処理を示す結果データＣ０を送受信手段１２４を介して送受信手段１１４に送信する。判断手段１１５は、この結果データＣ０にしたがいＩＣカード１２と端末１１とのセッションを終了させる。

【００３２】比較の結果、分離された識別データＣＥＲ２が識別データＣＥＲ１と一致しない場合には（Ｓ２０７でＮＯ）、上記認証コードＰＩＮ１、および、電文データＤ２は正しくないと判断する（Ｓ２１０）。すなわち、認証コードＰＩＮ１は当該セッション中のＩＣカード１２の認証コードではなく、電文データＤ２はホストコンピュータで処理された結果としての電文データＤ１と異なっていると判断する。したがって、この電文データＤ２をＩＣカード１２に書き込むことなく、異常処理を示す結果データＣ０を送受信手段１２４を介して送受信手段１１４に送信する。この結果、判断手段１１５がＩＣカード１２を端末１１から排出し（Ｓ２１１）、セッションを終了させる。この結果、ＩＣカード１２への不正な書き込みは防止される。

【００３３】以上、説明したように本実施例においては、電文データＤ１を、認証コードＰＩＮ１より生成した鍵データＫ１に従い暗号化し、暗号合成電文データＭＥを生成している。よって、暗号合成電文データＭＥは電文データＤ１に加えて認証コードＰＩＮ１の情報をも有していることになる。このため、本実施例に係るデータ処理方式は、従来のデータ処理方式にて行われていたように認証コードＰＩＮ１と電文データＤ１を別々に暗号化・復号化を行う必要がない。また、本実施例に係るデータ処理方式を従来のデータ処理方式と比較すると、

端末とＩＣカードとの間のデータの送受信は４回から２回へと、暗号化・復号化の回数は６回から２回へと減少している。したがって、本実施例によれば、端末とＩＣカードとの間のセッションに要する時間を、数ｓｅｃから数百ｍｓｅｃへと大幅に減少することができる。

【００３４】また、鍵データＫ１はＩＣカード毎に異なる認証コードＰＩＮ１を暗号化することにより生成されている。このため、仮に、一枚のＩＣカード１２の認証コードＰＩＮ１が第三者に知られたとしても、他のＩＣカード１２の鍵データＫ１は知られないため、他のＩＣカード１２のデータの機密性が低下することはない。よって、他のＩＣカードのデータの機密性までも損なわれることはなく、いわゆるセキュリティ・リスクによる被害を最小限に抑えることができる。さらに、第三者が他人のＩＣカード１２を取得した場合にも、第三者が該ＩＣカードの認証コードを知らなければデータの暗号化、復号化は不可能である。

【００３５】したがって、本実施例に係るデータ処理方式は、従来のデータ処理方式と比較してデータの機密性を低下させることなく、セッションに要する時間を短縮することができる。

【００３６】

【発明の効果】以上説明してきたように、本発明によればデータの機密性を低下させることなく処理時間を短縮できるデータ処理方式を提供することができる。

【図面の簡単な説明】

【図１】本発明の第１実施例に係るデータ処理方式を示す概略ブロック図である。

【図２】本発明の第１実施例に係るデータ処理方式の動作を示すフローチャートである。

【図３】従来のデータ処理方式の一例を示す概略ブロック図である。

【符号の説明】

１１	端末システム（送信側）
１２	ＩＣカード（受信側）
１１１	第１の暗号化手段
１１２	データ付加手段
１１３	第２の暗号化手段
１１４	送受信手段（送信手段）
１２１	復号化手段
１２２	データ分離手段
１２３	比較判断手段
１２４	送受信手段（受信手段）
Ｄ１	電文データ
Ｄ２	電文データ（復号電文データ）
ＰＩＮ１	認証コード
ＣＥＲ１	識別データ
ＣＥＲ２	識別データ（復号識別データ）
Ｍ１	合成電文データ
Ｍ２	合成電文データ（復号合成電文データ）

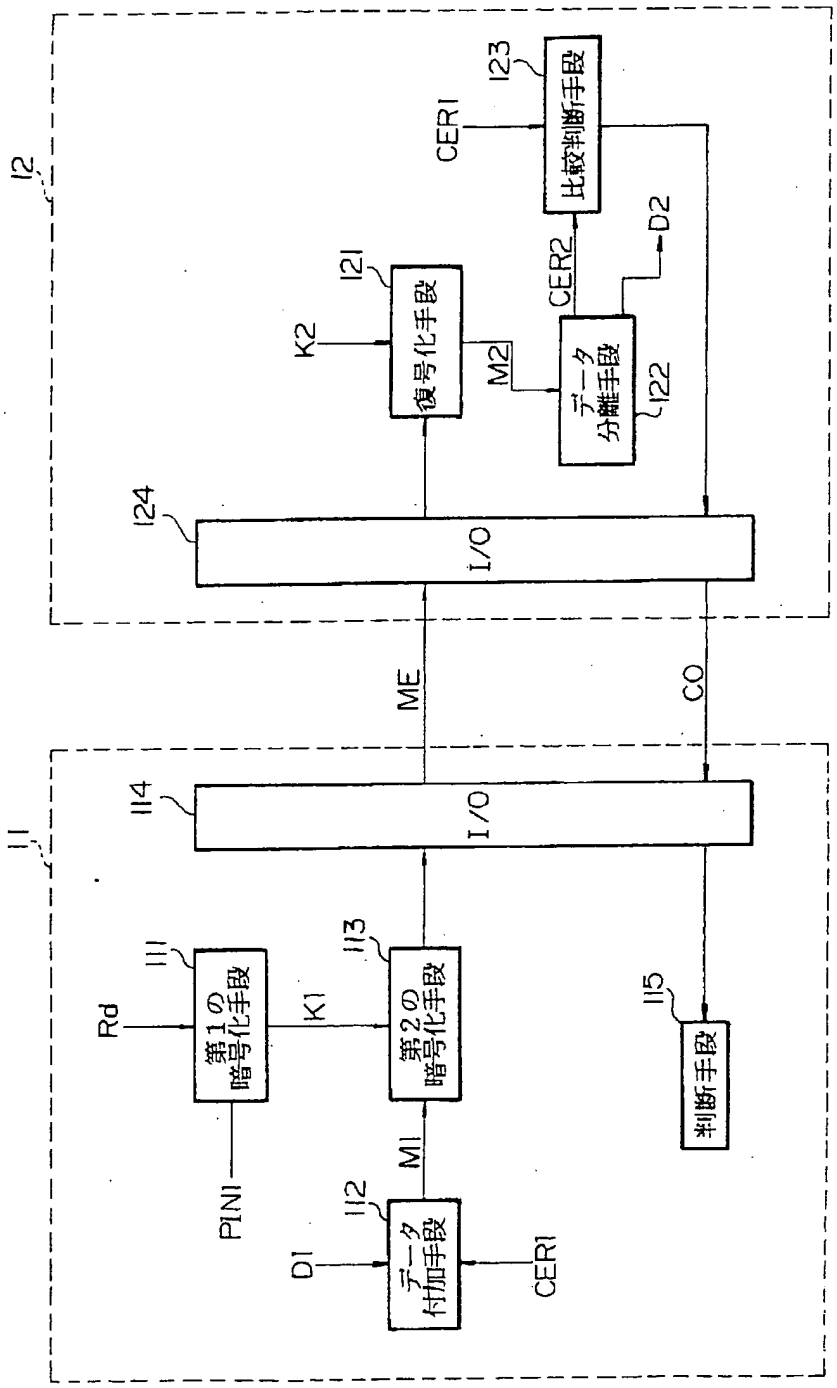
9

Rd　鍵データ（第1の鍵データ）
K1　鍵データ（第2の鍵データ）

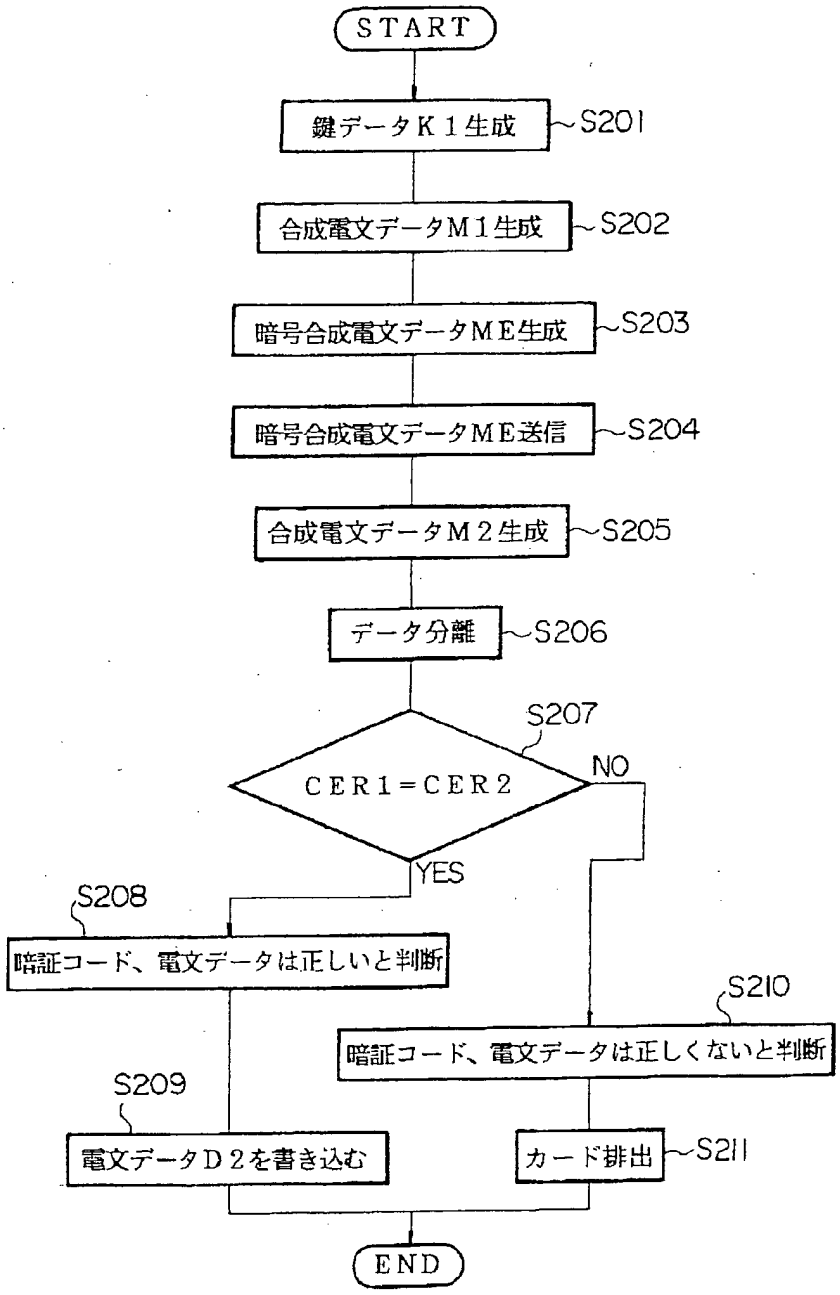
10

K2　鍵データ（第3の鍵データ）

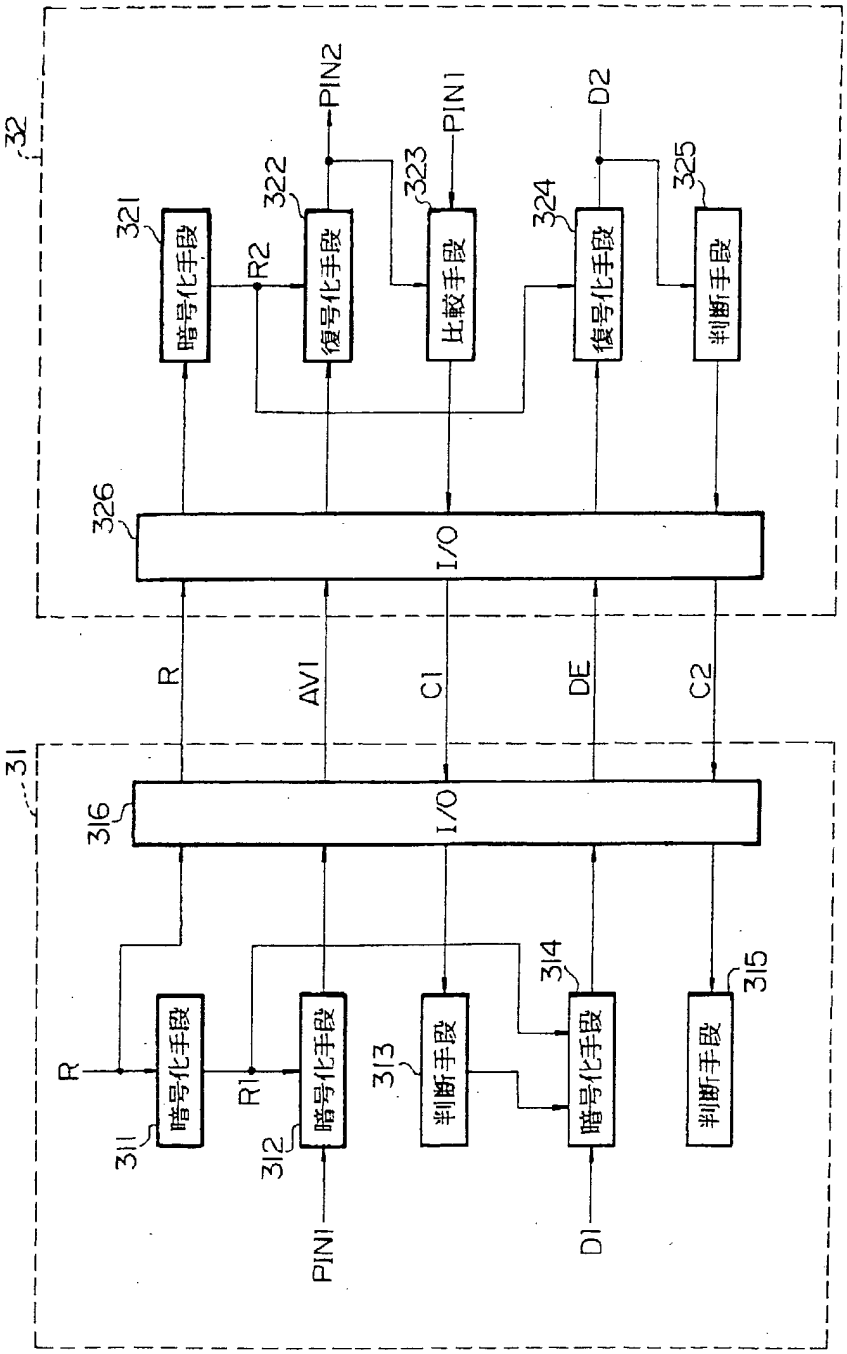
【図1】



【図2】


START
鍵データK1生成
S201
合成電文データM1生成
S202
暗号合成電文データME生成
S203
暗号合成電文データME送信
S204
合成電文データM2生成
S205
データ分離
S206
S207
CER1=CER2
NO
YES
S208
暗証コード、電文データは正しいと判断
S210
暗証コード、電文データは正しくないと判断
S209
電文データD2を書き込む
カード排出
S211
END

【図3】


32
321
暗号化手段
R2
322
復号化手段
PIN2
323
比較手段
PIN1
324
復号化手段
D2
325
判断手段
326
I/O
R
AV1
C1
DE
C2
31
316
I/O
R
311
暗号化手段
R1
312
暗号化手段
PIN1
313
判断手段
314
暗号化手段
D1
315
判断手段